

**UNITED STATES DISTRICT COURT FOR
THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION**

DONNA CURLING, et al.

Plaintiff,

VS.

BRAD RAFFENSPERGER, et al.

Defendant.

CIVIL ACTION FILE NO.:

1:17-cv-2989-AT

DECLARATION OF MATTHEW D. BERNHARD

MATTHEW D. BERNHARD declares, under penalty of perjury, pursuant to 28 U.S.C. § 1746, that the following is true and correct:

1. Based on the research that I have done regarding GEMS databases, including the inspection of two Georgia GEMS databases posted online in the public domain, I believe that it is highly unlikely that the GEMS database in the state of Georgia differs in any meaningful way from other databases that are already in the public domain. Even if the database is different from other known versions of the GEMS database, exposing the data in the database creates no more risk to which Georgia's voting system is already exposed.

2. The defendants' concerns about exposing the "structure" of the database are not well-formed, and a clear articulation of what specific structure they are concerned about is necessary in order to formulate a work plan that can address those concerns.

3. From discussion with Merritt Beaver, the Chief Information Officer for the Secretary of State, it seems as if the “structure” to which they are referring has to do with the specific identifiers associated with candidate, precincts, and so forth. This is the actual data contained within the database, and can be easily ascertained from multiple pieces in the voting system, including on voting machines which have been shown to be completely exposed to anyone in the vicinity of a precinct. Moreover, these data are generated in a repeatable, automated way that can be inferred from GEMS source code which is already in the public domain. Nothing about these identifiers is security critical, and it is highly unlikely that the version of GEMS used in the state of Georgia differs in the way it generates this data.

4. The state has also, in the same discussion, separately articulated a fear of exposing the overall structure of the database, i.e. the names of the tables and fields which are

stored in the database. This definition of “structure” is likely inconsequential, as these particular properties are already public in databases from other states and from the state of Georgia itself, all of which contain the exact same tables and fields. Furthermore, as the database is distributed to all 159 counties in Georgia and few security procedures are in place to guarantee that copies of the database stay on the county’s servers. It does not seem plausible that this definition of “structure” is a closely held secret by the state, and again the fields and tables within the database are already public knowledge.

PROPOSED WORK PLAN¹

5. Assuming that the GEMS databases as maintained by the state really are fundamentally different than prior known public versions of the database, even versions from the state itself, and assuming these differences comprise security-sensitive data or tables within the table, the following work plan as proposed by Plaintiffs’ brief ought to allay the states security concerns.

6. Plaintiffs' experts, along with lawyers, will obtain copies of the databases in controlled environments. The databases can be mailed as encrypted CDs, and experts can call the state to receive a password to decrypt the CDs, which is the same process already followed by the state to send databases to counties. CDs will be loaded onto air-gapped machines containing Microsoft Access, Microsoft Excel, as well as the Python programming language.

7. Plaintiffs' experts will use the tools on the air-gapped machine to examine the databases for obvious flaws, including but not limited to malformed data, contests that are not denoted in the database to be excluded from ballots, and so forth. Plaintiffs' experts will also compare between county databases for any obvious anomalies.

8. After agreement with Defendants on specific data to be shared, Plaintiffs' experts will extract data from the database to be reviewed by Plaintiffs and their analysts. By extracting specific information, for example cast vote records, exposure of the structure of the database can be avoided while also allowing plaintiffs to efficiently and effectively examine particular election data. Data that is expected to be extracted for external review by plaintiffs include, but is not limited to, the audit log (from the AuditLog table), candidate-to-candidate ID and type mappings (from the Candidate table), voting group data and identifiers (which candidates can appear in which races, and which races appear in which jurisdictions, from the CandVGroup table), and so on. The data in each of these tables will be copied out separately, and given to separate investigators.

9. Data will be transferred from the machine hosting the GEMS databases following the procedure outlined in the TTBR: new, removable storage media (CDs or USB sticks) will have the extracted data loaded onto them on the machine hosting the GEMS database and then

¹ Work plan adapted from California’s TTBR:

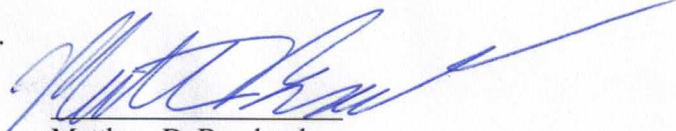
<https://votingsystems.cdn.sos.ca.gov/oversight/ttbr/source-code-security-plan.pdf>

transferred to plaintiffs' machines for examination. Once a media devices has been used, it may not be used again. No media already containing data will be connected to or opened by the machine containing the GEMS databases.

10. If, upon examination, the GEMS databases do not differ significantly in structure or contents from known public databases, experts will notify attorneys for the Plaintiffs to seek agreement with the approval of the Court to disclose the GEMS databases to Plaintiffs.

11. Any significant aberrations found by plaintiffs' experts or by external investigators will be documented, and this documentation will be made available to the court. Documentation will not be made public unless it is agreed that its disclosure would not pose significant harm to Georgia's election security.

This 3rd day of July, 2019.



Matthew D. Bernhard